cnet NEWS.COM TECH NEWS FIRST

CNET tech sites: | Price comparisons | Product reviews | Tech news | Dow

FRONT PAGE | ENTERPRISE SOFTWARE | ENTERPRISE HARDWARE | SECURITY | NETWORKING | PERSONAL TECH

SAVED STORIES 0 SEAR

Powerful Technology. Powerful Savings.
Save now with our weekly specials.
Mor
D
Dell | Sr

News.com special report

WHY HACKERS ESCAPE

Organized, well-financed criminals stay a step ahead of the law

By Greg Sandoval
Staff Writer, CNET News.com
May 14, 2002, 4:00 a.m. PT

The nightmare for Ecount, an online gift certificate service, began last year when a hacker broke in to the company's system and stole personal information belonging to its customers.

HACKERS SWAP CREDIT CARD TIPS
Click here >

Nine months later, the criminal is still at large. The thief has brazenly taunted executives with repeated e-mails while staying ahead of investigators, deftly wiping away his electronic fingerprints and covering his tracks at every turn.

"We're sick to death of hearing from him," Ecount Chief Executive Matt Gillin said of the intruder, who has offered to return the information for a fee.

Although law enforcement agencies are quick to trumpet their occasional victories against cybercriminals, they are rarely able to track down hackers sophisticated enough to pull off such complicated heists. Few hackers of this caliber are arrested, and fewer still spend time behind bars.

CLEAN GETAWAY

Sophisticated hackers erase their tracks, making it nearly impossible to hunt them down. Here's how one hacker might get away with a list of credit card numbers.

The resulting frustration for investigators, companies and consumer victims raises a question that has persisted for years: Why are hackers able to elude capture so easily? The answer, according to security analysts and fraud investigators, is that the Internet has bred an elite class of criminals who are organized, well funded and far more technologically sophisticated than

Protect you against onl

Although it's impo guarantee online experts say cons help protect them following a few si

- Use a credit car a debit card.
- Use only one ca online.
- Keep the credit
- Shop at familiar
- Make sure the s encryption techno
- Choose passwo aren't easy to gu

Related stories

Anatomy of a

New tool helps evade detectio

most law enforcement officials.

"It's a world-class business," said Richard Power, editorial director of the Computer Security Institute, a private research firm that tracks electronic crime. "Al-Qaida and serious narcotic terrorists are using credit card fraud to finance their groups."

Fraud cost e-tailers $700 million in lost merchandise last year, says Avivah Litan, a financial analyst for research firm Gartner. Some large Internet retailers have software that screens transactions and refuses to sell to customers who appear suspicious. Litan estimates that this costs Web stores between 5 percent and 8 percent of sales.

A Gartner study also shows that 5.2 percent of online shoppers have been victimized by credit card fraud and 1.9 percent by identity theft.

"These are huge numbers. This is scary stuff," Litan said. "The Internet has got an albatross around its neck."

Special report
Cracking the nest egg ▶
Hackers find fortunes
in online banking accounts

Skilled hackers shake off investigators by shuttling between multiple servers before launching an attack. After fleeing a targeted site with credit card numbers or other bounty, the intruders immediately begin deleting the log files of each server they have passed through, eliminating any record that they were there.

It is the equivalent of "vacuuming up the crime scene," said independent fraud investigator Dan Clements, who runs a Web site devoted to catching hackers called CardCops.com. Only about 10 percent of active hackers are savvy enough to work this way consistently, he said, but they are almost always successful.

Having grown up with the breakneck pace of "Internet time," hackers of this digital generation use speed as a primary weapon. As with all criminal investigations, pursuing online suspects means time-consuming records searches that often require subpoenas--a process that can give hackers an insurmountable advantage.

FBI agents can swiftly get subpoenas from the courts but often lose critical time trying to serve them. Agents can spend days sorting through digital smoke screens created by multiple servers, requiring agents to obtain and serve multiple subpoenas.

"AL-QAIDA AND SERIOUS NARCOTIC TERRORISTS ARE USING CREDIT CARD FRAUD TO FINANCE THEIR GROUPS."

-Richard Power,
editorial director,
Computer Security Institute

In the meantime, valuable evidence is often lost, and by then, hackers are long gone.

The federal government is taking steps to improve its fight against criminal activity online. FBI Director Robert S. Mueller created a new cybercrime unit in December, and the Bush administration has added 50 new federal prosecutors to address the problem nationwide.

Still, few believe that these measures will eradicate a problem that's become so deeply entrenched. The FBI confirmed, for example, that no arrests have been made in any of six recent high-profile cases reviewed by CNET News.com:

- **Playboy.com**: An intruder slipped past the Web site security systems of the adult entertainment company last November and obtained the personal information of an undisclosed number of customers of the site's e-commerce store. The hacker notified customers that he or she had pilfered the information and, as proof, gave them their credit

Cloaked code
corporate secu

Hackers find n
bilk eBay user

Pacific Rim a
for hack attack

Tools for a mo
Internet

Deciphering th
myth

Playboy says
stole custome

Hacker disclos
after demands

As Net fraud g
do e-tailers' fe

Hack at Amaz
service expos
thousands

Online stores
the doors

FBI looking int
questionable c
charges

Company say
try exposes th
of card numbe

Hacker attack
string of online
card thefts

AmEx, Discov
to replace card
security breac

FBI probes ex
case at CD sto

News arou
the Web

U.S. hacker se

card numbers.

- **Ecount**: Last summer, a hacker circumvented the Internet defenses of the Philadelphia-based company's gift certificate service and notified customers of the breach in an e-mail that included their home addresses. The hacker then demanded $45,000 from the company to keep him from exposing the personal information of 350,000 customers.

- **Egghead.com**: A hacker infiltrated the e-tailer's system in December 2000. After three weeks of investigation, the company said the intruder did not obtain the personal information of its 3.7 million customers, but many banks said they spent millions of dollars to issue new credit cards in the meantime.

- **Creditcards.com**: Also in December 2000, a hacker broke in to systems maintained by the company, which enables merchants to accept payments online, and made off with about 55,000 credit card numbers. The hacker tried to extort the company and, when executives refused to pay, exposed the numbers by posting them on the Web.

- **Western Union**: In September 2000, a hacker exploited an opening in the Web site of the financial services company and got away with more than 15,000 credit card numbers. Human error left "performance management files" open on the site during routine maintenance, allowing the hacker access.

- **CD Universe**: About 350,000 credit card numbers were stolen from the online music company in January 2000, one of the first large-scale hackings of its kind. The thief, identified only as "Maxus," held the card numbers hostage and demanded a $100,000 ransom. When the company refused, the hacker posted the numbers on a Web site.

Without commenting on these specific cases, law enforcement officials say many online merchants may be partly to blame for the lack of arrests because they do not devote enough resources to prevent intrusion or facilitate investigations in the event of a crime.

"If there is any message to get out there, it would be for companies to upkeep their antivirus and firewall software," said Laura Bosley, a spokeswoman for the FBI's Los Angeles field headquarters.

UNSOLVED HACKS

The people who stole credit card numbers from these major online merchants are still at large.

Company	Date	What they stole; additional crimes
Playboy.com	Nov 2001	Undisclosed number of credit card numbers; extortion
Ecount	Aug 2001	Personal customer information; extortion
Western Union	Sep 2000	15,000 card numbers
Creditcards.com	Dec 2000	55,000 card numbers exposed on the Web; extortion
Egghead.com	Dec 2000	3.7 million credit cards threatened*
CD Universe	Jan 2000	350,000 card numbers posted online; extortion

* Egghead announced that a hacker had accessed its computer system, "potentially including (its) customer databases."

Source: CNET News.com research

Jennifer Granick, litigation director at the Stanford Law School Center for Internet and Society, said security is often neglected by companies more interested in making a quick buck.

E-commerce companies "rushed online during the dot-com boom, and they saw the money that was to be had and didn't give a thought to security," she said. "They were too busy trying to capture eyeballs to secure their sites."

Even if they have fortified their Web sites against attack, many companies are still unaware of the importance of preserving evidence if a crime occurs--ignorance that can kill any hope of catching a perpetrator, said Bruce Smith, an investigator for Pinkerton Consulting & Investigations and a former FBI agent who worked on computer crime cases

in worldwide c
The Washington

White-collar crimefighters
Business 2.0

Experience is security start-u
Washtech.com

Lab will help F high-tech case
The Kansas City St

The saint of e-commerce? N
FBI's "Gotcha" pag

Russian comp hacker convic
U.S. Department o

Editors: Mike Yam Wilson, Lara Wrigh Balderama
Design: Ellen Ng
Production: Ben H

for six years.

Frequently, Smith said, agents will scan the Web logs of a hacked company only to find a blank record that leaves the intruder's trail stone cold. Sometimes, he said, the shopkeeper accidentally destroys the logs, covering the hacker's tracks with other records. More often, the online store never turns on the logging feature to begin with because it could slow a Web site's performance.

"You cross your fingers when you start looking at the logs," Smith said. "Sometimes you get lucky, sometimes not."

News.com video

Hackers expose credit card numbers
Chris Rouland, Internet Security Systems
December 13, 2000

Moreover, precious time can be lost when companies hesitate to contact authorities immediately after an intrusion. The reason for the delay is often rooted in business, not justice.

"Fear," Smith said. "They're reluctant to admit that they've been victimized. You can imagine the bad press. Here's someone who's telling clients their information is safe at the same time their site is getting hacked."

Security experts blasted Egghead for taking weeks to investigate whether the personal information of its customers had been compromised. A company with good logging capability should have been able to determine the extent of the intrusion within a few days, security specialists said, perhaps saving banks a cost of between $5 and $25 for each new credit card issued out of precaution.

"I think there was some things that we wished we did before the attack," said Jeff Sheahan, the former chief executive of Egghead. "We thought we had a tight oversight system. We asked ourselves how we missed this. It was just focusing on other things and not sensing that there was a big enough risk."

The investigation was expensive for Egghead, but the intrusion exacted a much higher price in the form of lost confidence among its customers. "When you're an e-commerce business, trust is important. I don't think there is any doubt that trust level took a hit to some degree," Sheahan said.

E-COMMERCE COMPANIES ARE "RELUCTANT TO ADMIT THAT THEY'VE BEEN VICTIMIZED. YOU CAN IMAGINE THE BAD PRESS."

-Bruce Smith, Investigator, Pinkerton Consulting & Investigations

Other online merchants would do well to learn from Egghead's mistakes, for the number of hackings is growing. To gauge this trend, CardCops' Clements posted fake credit card numbers on the Web and then spread the word at sites popular with "carders"--those who traffic in stolen credit cards--that a Web site had accidentally divulged the information.

In less than a half-hour, the site had 74 visitors from 31 countries. Within a couple of days, the number of visitors had grown to 1,600. No one can say how many came to the site with criminal intent, but Clements believes most did.

"There's a war raging online," he said, "and the bottom line is that law enforcement is losing." ▨

How to advertise | Send us news tips | Contact us | Corrections | XML | Linking policy | Licensing | Mobile | News

FRONT PAGE | ENTERPRISE SOFTWARE | ENTERPRISE HARDWARE | SECURITY | NETWORKING | PERSONAL TECH

Featured services: **BNET: Business White Papers** | **Free magazine trial** | **CNET's Digital Living** | **Find tech j bs** | **Hot D**

CNET.com | **CNET Download.com** | **CNET News.com** | **CNET Reviews** | **CNET Shopper.com**

GameSpot | **mySimon** | **Search.com** | **TechRepublic** | **ZDNet** | **International Sites**